УДК [351.74(100):004.9](075.8)
МОГІЛЕВСЬКИЙ Леонід Володимирович,
доктор юридичних наук, професор, заслужений юрист України,
проректор Харківського національного університету внутрішніх справ
https://orcid.org/0000-0002-6994-6086

КІБЕРЗЛОЧИННІСТЬ У ПРОЄКТІ ЄВРОПОЛУ SOCTA

Постійний моніторинг та аналіз стану і трендів у сфері організованої злочинності, особливо кіберзлочинності, є невід'ємною частиною у плануванні діяльності правоохоронних структур. Надважливим кроком у розвитку цього напряму діяльності й інтеграції зусиль правоохоронних органів країн Європейського Союзу є проєкт SOCTA.

SOCTA (англ. SOCTA – Serious and Organized Crime Threat Assessment) розробляється і публікується Європолом у співпраці з консультативною групою SOCTA, до складу якої входять

держави члени ЄС, агентства ЄС, Європейська комісія та Генеральний секретаріат Ради за підтримки європейських країн партнерів та організацій Європолу. Методологію схвалено Радою міністрів юстиції та внутрішніх справ ЄС.

Проєкт Європолу SOCTA охоплює:

– підготовку та затвердження детальних вимог одержувача даних;

– підготовку та схвалення методології;

– визначення вимог до збору оперативних даних;

– збір даних;

– аналіз даних (у т. ч. і Великих Даних);

– складання звіту SOCTA, включно зі списком основних загроз і ризиків;

– презентація результатів і рекомендованих пріоритетів.

У процесі аналізу особлива увага приділяється чотирьом такими елементам:

1) галузі / види тяжкої та організованої злочинної діяльності;

2) організовані злочинні групи / мережі та поодинокі правопорушники, причетні до тяжких злочинів;

3) середовище: уразливості, можливості та інфраструктура;

4) наслідки і шкода.

SOCTA розвиває Національну модель організації розвідувальної діяльності Управління Організації Об'єднаних Націй з наркотиків і злочинності, яка ґрунтується на дев'яти аналітичних методах і продуктах:

1) системний аналіз злочинної практики – це загальний термін для декількох видів аналізу, включно з виявленням тенденцій та аналізом «гарячих точок»;

2) аналіз демографічних / соціальних тенденцій, що оцінює вплив соціально-економічних і демографічних змін на злочинність, а також демографічні зрушення і ситуацію з безпритульністю;

3) мережевий аналіз, що оцінює напрямок, частоту і силу зв'язків між спільниками у злочинній мережі;

4) аналіз потенційного ринку збуту, що оцінює кримінальний ринок щодо певного товару, такого як наркотики або проституція;

5) аналіз сфери злочинного бізнесу, визначає бізнес модель і методи, використовувані окремими злочинцями або ОЗУ;

6) аналіз ризиків, що оцінює масштаб ризиків або загроз, створюваних правопорушниками або організаціями для окремих потенційних жертв, поліції і громадськості;

7) аналіз цільового профілю, що описує злочинця, його сильні та слабкі сторони, спосіб життя, зв'язки, злочинну діяльність і точки можливого заходу у життя цільового злочинця;

8) оцінка оперативної розвідувальної діяльності, що розглядає відповідність збору інформації раніше узгодженим завданням і виявляє прогалини в зусиллях із проведення розвідувальних дій (у великомасштабних проєктах та операціях);

9) аналіз результатів, що оцінює ефективність діяльності правоохоронних органів і контролює перебіг виконання планів.

У межах підготовки доповіді Європол в 2015–2017 рр. здійснив найбільший в історії аналіз Великих Даних щодо серйозної та організованої злочинності в ЄС. Європол використовував тисячі доповідей, інформаційних довідок та файлів держав-членів, оперативних і стратегічних партнерів. У доповіді в повному обсязі відображено дані оперативної розвідки, що зберігаються в базах даних Європолу. У результаті цього в межах підготовки доповіді вдалося надати найбільш докладну оцінку характеру і масштабів загроз злочинності, що стоять перед ЄС і його державами-членами.

У доповіді Європолу зазначено, зокрема, що «злочинці швидко впроваджують і інтегрують нові технології в свій modus operandi або створюють абсолютно нові бізнес моделі навколо них. Використання нових технологій ОЗУ впливає на злочинну діяльність по всьому спектру серйозної та організованої злочинності. В першу чергу, це відноситься до цифрового криміналу, який широко використовує масштабування онлайн торгівлі і повсюдне поширення зашифрованих каналів зв'язку».